The idea of the Arithmetica

Hajime Mashima

June 1, 2014

Abstract

During the 360 years of Fermat's last theorem is to be proved, this proposition was the presence appear full-length novel in "The Lord of the Rings", such as the "One Ring". And finally in 1994, it was proved completely by Andrew Wiles. However interesting proof is Fermat has been is still unknown. This will be assumed in the category of algebra probably.

introduction

Natural number X,Y and Z solution of 3 or more that this equation holds $X^n + Y^n = Z^n$ does not exist. Fermat is proven for the conditions of n = 4. It is sufficient if n is examining the conditions of prime numbers greater than or equal to 3 for this.

Theorem 1 *Triangle the hypotenuse of Pythagorean theorem is z, can be expressed by the following relation by using the l and m.*

$$\left(l^2 - m^2\right)^2 + 2^2 \left(lm\right)^2 = \left(l^2 + m^2\right)^2$$

$$\begin{aligned} x^2 &= \left(l^2 - m^2\right)^2 \\ y^2 &= 2^2 \left(lm\right)^2 \\ z^2 &= \left(l^2 + m^2\right)^2 \\ (xyz &\neq 0) \end{aligned}$$

To simplify the algebra as a real number M, and N.

$M, N \in \mathbb{R} \qquad l^2 = M,\ \ m^2 = N$

$$\left(M - N\right)^2 + 2^2 MN = \left(M + N\right)^2$$

Put $\quad X,Y,Z \in \mathbb{N} \quad prime\ \ number = p \geq 3$

$$\begin{aligned} X^p &= (M-N)^2 \\ Y^p &= 2^2 MN \\ Z^p &= (M+N)^2 \end{aligned}$$

$(XYZ \neq 0)$

Add the following conditions. $\quad X,Y,Z \in even\ \ number$

$$\begin{aligned} X^p &= 2^p X_1^p \\ Y^p &= 2^p Y_1^p \\ Z^p &= 2^p Z_1^p \end{aligned}$$

$(X_1, Y_1, Z_1 \in \mathbb{N})$

$MN = 2^{p-2} Y_1^p \in \mathbb{N}$

Thus M,N is a rational or irrational both.

1 M,N is a condition of both rational

$X^p = 2^p X_1^p \ \ , \ \ Z^p = 2^p Z_1^p$
$M-N, M+N \in evennumber$, and it will be a divisor of $2^{\frac{p+1}{2}}$ at least.

Consequently, $Y_1^p \in even\ \ number$ so $X_1^p \ \ , \ \ Z_1^p \in even\ \ number.$ (1)

2 M,N is a condition of both irrational

$$\begin{aligned} MN &= 2^{p-2} Y_1^p \\ &= 2^{p-2}\left(Z_1^p - X_1^p\right) \\ &= 2^{p-2}\left(\sqrt{Z_1^p} + \sqrt{X_1^p}\right)\left(\sqrt{Z_1^p} - \sqrt{X_1^p}\right) \end{aligned}$$

$X^p = 2^p X_1^p \ \ , \ \ Z^p = 2^p Z_1^p$

$$M = \left(\sqrt{2^{p-2} Z_1^p} + \sqrt{2^{p-2} X_1^p}\right) \quad N = \left(\sqrt{2^{p-2} Z_1^p} - \sqrt{2^{p-2} X_1^p}\right) \quad (M > N)$$

Put$(c,d \in odd\ \ number \qquad h,i \in \mathbb{N})$
$M = 2^{\frac{h}{2}} c^{\frac{1}{2}} + 2^{\frac{i}{2}} d^{\frac{1}{2}} \qquad N = 2^{\frac{h}{2}} c^{\frac{1}{2}} - 2^{\frac{i}{2}} d^{\frac{1}{2}} \qquad$ (I)

In addition, assuming that there is no difference and sum,

Put$(U, V \in odd\ \ number)$

$M = 2^{\frac{l}{2}}U \qquad\qquad N = 2^{\frac{m}{2}}V \qquad\qquad (\mathrm{II})$

$MN = 2^{p-2}Y_1^p = 2^{\frac{l+m}{2}}UV \in \mathbb{N}$

M, N because irrational both,therefore$(l, m \in odd\ \ number)$.

2.1 Conditions of (II)

2.1.1 Conditions of $(Y_1^p \in odd\ \ number)$

$Y_1^p = Z_1^p - X_1^p$

Z_1^p, X_1^p is the relationship of "odd and even" or "even and odd".

Z_1^p and X_1^p are assumed to be coprime.Common divisor $R^p\,(\in odd\ \ number)$, if present in the Z_1^p and X_1^p , is included as a common divisor of R^p also Y_1^p. $(\frac{Y_1^p}{R^p} \in \mathbb{N})$

It is possible to remove common divisor, it is sufficient Z_1^p and X_1^p is examining the conditions of coprime.

$MN = 2^{p-2}Y_1^p = 2^{\frac{l+m}{2}}UV \qquad (p = \frac{l+m}{2} + 2 \qquad Y_1^p = UV)$

Proposition 2 $l > m \qquad \frac{l+m}{2} > m\ (l, m \in odd\ \ number \quad U, V \in odd\ \ number)$

$$\underline{odd\ \ number = 2^{\frac{l-m}{2}+2}X_1^p}$$

$$\begin{aligned} X^p &= (M-N)^2 \\ &= M^2 + N^2 - 2MN \\ &= 2^l U^2 + 2^m V^2 - 2\cdot 2^{\frac{l+m}{2}}UV \\ &= 2^m\left(2^{l-m}U^2 + V^2 - 2\cdot 2^{\frac{l-m}{2}}UV\right) \\ &= 2^m\,(odd\ \ number) \end{aligned}$$

$$X^p = 2^m\left(2^{\frac{l-m}{2}+2}X_1^p\right)$$

$$odd\ \ number \neq 2^{\frac{l-m}{2}+2}X_1^p \tag{2}$$

Lemma 3 $l = p-2 \qquad m = p-2\ (l, m \in odd\ \ number \quad U, V \in odd\ \ number)$

<u>*Other things being does not hold all applies the infinite descent.*</u>

$$X^p = (M-N)^2 = \left(2^{\frac{p-2}{2}}U - 2^{\frac{p-2}{2}}V\right)^2 = 2^{p-2}(U-V)^2$$

$$\begin{aligned} 2^2 X_1^p &= (U-V)^2 & (U>V) \\ 2\sqrt{X_1^p} &= U-V & \cdots① \end{aligned}$$

$$Z^p = (M+N)^2 = \left(2^{\frac{p-2}{2}}U + 2^{\frac{p-2}{2}}V\right)^2 = 2^{p-2}(U+V)^2$$

$$\begin{aligned} 2^2 Z_1^p &= (U+V)^2 & (U>V) \\ 2\sqrt{Z_1^p} &= U+V & \cdots② \end{aligned}$$

X_1^p, Z_1^p is a square number $U \pm V$ because it is a natural number.

$X_1^p = (X_{II}^p)^2 \quad Z_1^p = (Z_{II}^p)^2 \quad (X_{II}^p, Z_{II}^p \in \mathbb{N})$

simultaneous equation:①±②

$$U = Z_{II}^p + X_{II}^p \qquad V = Z_{II}^p - X_{II}^p$$

If U,V is not a coprime, and a common divisor r($\in odd\ \ number$).

$$\begin{aligned} U = Z_{II}^p + X_{II}^p &= rf & \cdots③ \\ V = Z_{II}^p - X_{II}^p &= rg & \cdots④ \end{aligned}$$
$$(U, V \in odd\ \ number \qquad f, g \in odd\ \ number)$$

simultaneous equation:③±④

$$\begin{aligned} 2Z_{II}^p &= r(f+g) \\ 2X_{II}^p &= r(f-g) \end{aligned}$$

X_{II}^p, Z_{II}^p comprises a common divisor r. butX_{II}^p, Z_{II}^pmust also be coprime X_1^p, Z_1^p is coprime. Thus U, V is coprime.

Theorem 4 $(Y_1^p = UV)$ *U, V is at a coprime, which is a power of a prime number.*

$$U = U_{II}^p \ , \ V = V_{II}^p \qquad Y_1^p = (U_{II}V_{II})^p$$

Substitute U_{II}^p, V_{II}^p for ③,④.

$$U_{II}^p = Z_{II}^p + X_{II}^p \qquad V_{II}^p + X_{II}^p = Z_{II}^p \tag{3}$$

2.1.2 Conditions of $(Y_1^p \in even\ \ number)$

It is equivalent to X_1^p because it is odd number.

$MN = 2^{p-2}X_1^p = 2^{\frac{l+m}{2}}UV \qquad (p = \frac{l+m}{2} + 2 \qquad X_1^p = UV)$

Proposition 5 $\qquad x^p + y^p = z^p$
x and z is a square number, both when this condition is satisfied.

Put $\quad a^p, b^p, c^p \in \mathbb{R} \qquad prime\ \ number = p \geq 3$

$$a^p + b^p = c^p$$

$$2^2 a^p b^p = (c^p)^2 - (a^p - b^p)^2$$

Put $\quad a^p = 2^{-1}a_1^p \qquad b^p = 2^{-1}b_1^p \qquad\qquad 2^{-1}a_1^p + 2^{-1}b_1^p = c^p$

$$\begin{aligned} a_1^p b_1^p &= (c^p)^2 - \left(2^{-1}a_1^p - 2^{-1}b_1^p\right)^2 \\ a_1^p b_1^p &= \left(c^2\right)^p - \left(\frac{a_1^p - b_1^p}{2}\right)^2 \\ \left(\frac{a_1^p - b_1^p}{2}\right)^2 + (a_1 b_1)^p &= \left(c^2\right)^p \end{aligned}$$

Conditions; $\quad (c^p \ ,\ \ a_1^p b_1^p \in \mathbb{N} \qquad a_1^p \ ,\ \ b_1^p \in$irrational)

Put $\quad d \ ,\ \ e \in \mathbb{N}$

$$\begin{aligned} a_1^p &= d + e^{\frac{1}{2}} \\ b_1^p &= d - e^{\frac{1}{2}} \end{aligned}$$

$$a_1^p b_1^p = d^2 - e$$

$$\begin{aligned} a^p &= 2^{-1}d + 2^{-1}e^{\frac{1}{2}} \qquad \left(a^p = 2^{-1}a_1^p\right) \\ b^p &= 2^{-1}d - 2^{-1}e^{\frac{1}{2}} \qquad \left(b^p = 2^{-1}b_1^p\right) \end{aligned}$$

$$a^p + b^p = d = c^p \qquad \cdots⑤$$

Put $\quad a^p = 2^{-2}a_2^p \qquad\qquad 2^{-2}a_2^p + b^p = c^p$

$$\begin{aligned}
a_2^p b^p &= (c^p)^2 - \left(2^{-2}a_2^p - b^p\right)^2 \\
a_2^p b^p &= \left(c^2\right)^p - \left(\frac{a_2^p - 4b^p}{4}\right)^2 \\
\left(\frac{a_2^p - 4b^p}{4}\right)^2 + (a_2 b)^p &= \left(c^2\right)^p
\end{aligned}$$

Conditions; $\quad (c^p \ , \ a_2^p b^p \in \mathbb{N} \qquad a_2^p \ , \ b^p \in$irrational)

Put $\quad j \ , \ k \in \mathbb{N}$

$$\begin{aligned}
a_2^p &= j + k^{\frac{1}{2}} \\
b^p &= j - k^{\frac{1}{2}}
\end{aligned}$$

$$a_2^p b^p = j^2 - k$$

$$a^p = 2^{-2}j + 2^{-2}k^{\frac{1}{2}} \qquad \left(a^p = 2^{-2}a_2^p\right)$$

$$a^p + b^p = \frac{5}{4}j - \frac{3}{4}k^{\frac{1}{2}} = c^p \neq \mathbb{N}$$

As general conditions; $\quad (c^p \ , \ a_0^p b_0^p \in \mathbb{N} \qquad a_0^p \ , \ b_0^p \in$irrational)

Put $\quad j \ , \ k \in \mathbb{N} \qquad a^p = 2^q a_0^p \qquad b^p = 2^r b_0^p \qquad (q + r = -2 \ , \ q \neq r)$

$$\begin{aligned}
a^p &= 2^q j + 2^q k^{\frac{1}{2}} \\
b^p &= 2^r j - 2^r k^{\frac{1}{2}}
\end{aligned}$$

$$a^p + b^p = \left(2^q + 2^r\right) j - \left(2^q - 2^r\right) k^{\frac{1}{2}} = c^p \neq \mathbb{N}$$

By referring to the ⑤, It is a contradiction if c^p is a natural number. Therefore,

$$a^p + b^p = d = c^p \neq \mathbb{N} \qquad \left(2^{-1}a_1^p = 2^{-2}a_2^p \qquad 2^{-1}b_1^p = b^p\right)$$

Conditions; $(c^p \ , \ a_2^p b^p \in \mathbb{N} \qquad a_2^p \ , \ b^p \in$rational)

$$\left(\frac{a_2^p - 4b^p}{4}\right)^2 + (a_2 b)^p = \left(c^2\right)^p \qquad \frac{a_2^p - 4b^p}{4} \in \text{rational}$$

$$\alpha^p + \beta^p = \gamma^{2p} \qquad (\alpha \ , \ \beta \ , \ \gamma \in \mathbb{N})$$

Therefore, a square number also α when this condition is satisfied. $\cdots$⑥

$$x^p + y^p \quad = \quad z^p \quad \text{(x, y and z are disjoint.)}$$

And multiplied by z^p to both sides.

$$z^p x^p + z^p y^p \quad = \quad z^{2p}$$

By applying the ⑥, since "$z^p x^p$" is also a square number,

$$x^p = \left(x_1^p\right)^2 \ , \ z^p \quad = \quad \left(z_1^p\right)^2$$

$$\left(x_1^2\right)^p + y^p \quad = \quad \left(z_1^2\right)^p \quad (x_1\text{, y and } z_1 \text{ are disjoint.})$$

By referring to the (3),

$$U_{II}^p = Z_{II}^p + X_{II}^p \qquad V_{II}^p + X_{II}^p = Z_{II}^p$$

$$(2U_{II})^p = (2Z_{II})^p + (2X_{II})^p \qquad (2V_{II})^p + (2X_{II})^p = (2Z_{II})^p$$

$$(2Z_{II})^p < Z^p = (2Z_1)^p \qquad (2X_{II})^p < X^p = (2X_1)^p$$

Thus the lemma has been shown.

$$x^n + y^n \neq z^n \qquad (xyz \neq 0 \quad n \geq 3)$$